

REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

The present claims have been revised to overcome the issues prompting the rejections of claims 1 and 13 under 35 USC §112, second paragraph.

Claims 1, 2, 7, 8, and 13 have been amended to replace the expressions "pipe" and "communications pipe" with the expression "established communications pipe." Claims 1 and 2 have been amended to replace the expression "second remote computer" with "subsequent remote computer," and claim 13 has been amended to replace the phrase "generating PSD algorithm transfer command" with the expressions: (1) "wherein said PSD comprises an internal PSD algorithm" and (2) "generating a command for requesting a transfer of said internal PSD algorithm." Claims 14 to 17 have been amended to clarify their dependency from claim 13. These changes serve to clarify the claims and are non-narrowing. Therefore, no estoppel is deemed attachable to these changes.

Claims 1, 2, 7, 8, and 13-17 have been amended to better define the subject matter Applicants regard as the invention. Support for the features added to the claims is provided in claims 1 and 20 of U.S. patent application number 09/844,246, the

disclosure of which is incorporated into the present application by reference.

Claim 7 was rejected, under 35 USC §102(e), as being anticipated by Audebert (US 6,694,436). Claims 1-6 and 8-17 were rejected, under 35 USC §103(a), as being unpatentable over Audebert in view of Uhler et al. (US 2001/0039587). Applicants respectfully traverse the rejections.

The applied Audebert patent and the subject matter of the present application were commonly owned at the time that the present invention was made. Accordingly, under 35 USC §103(c), Audebert does not qualify as a 35 USC §103(a) reference against the present claimed invention. Therefore, withdrawal of this rejection is warranted.

Turning now to the 35 USC 102(e) rejection, the Applicants traverse based on the following points.

In the present claimed invention, as defined by new independent claims 1, 2, 7 and 13, when an APDU is desencapsulated from an incoming message packet, it is routed to the personal security device by the local client, without checking of its integrity or origin. This provides an advantage of making the local client completely transparent in the transmission of data between the remote server and the personal security device through the communications pipe.

In contrast, Audebert describes a system and method for performing secure electronic transactions, and especially authentication (col. 9, line 56). It is suited for transferring data between a first remote computer system (S sec) and a PSD 31 using a local client (the terminal module 1) as a communication host for said PSD.

More particularly, this method comprises (see figure 2B):

generating an authentication challenge on the first remote computer system (S sec) in a proper format for processing by the PSD 31 (column 13, lines 4-5 and lines 46-48),

encrypting said authentication challenge and transmitting it to said PSD via a secure channel CS (column 13, line 48 and column 12, lines 58-63),

decrypting said encrypted authentication challenge by the terminal module 1, before being transferred to the PSD (secure channel CS),

generating an authentication response by said PSD 31 using the authentication challenge and at least one internal PSD algorithm (column 13, lines 49-51),

encrypting said authentication response and transmitting it to the first remote computer system via the secure channel CS (column 13, line 48 and column 12, lines 58-63), and

decrypting said encrypted authentication response by the first remote computer system (secure channel CS).

Moreover, it is described that commands sent by the first remote computer system S sec are "routed" to the PSD (column 13, lines 7-11). It is also stated in another part of the document that, in one embodiment, a high level request sent by an application server can contain a single elementary command to be transferred to the personal security device, for example, an APDU in the case of a smart card" (see col. 10, lines 7-11). This can be considered as reproducing the feature according to which the local client comprises means for receiving incoming message packets from an application server (for instance S sec), separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to the PSD through the PSD interface.

But it appears that in the system as described in Audebert, when an APDU is desencapsulated from an incoming message packet, before being transferred to the personal security device by the local client, the filter F always checks the integrity and the origin of the incoming message packet (column 10, lines 7 to 14).

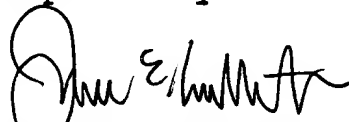
As noted above, in contrast to Audebert, new independent claims 1, 2, 7 and 13 define that, when an APDU is desencapsulated from an incoming message packet, it is routed to

the personal security device by the local client, without checking of its integrity or origin. This makes the local client completely transparent in the transmission of data between the remote server and the personal security device through the communications pipe.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



James E. Ledbetter

Registration No. 28,732

Date: April 19, 2005
JEL/DWW/att

Attorney Docket No. L741.01102
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200